(6)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-147898

(43)Date of publication of application : 29.05.2001

(51)Int.Cl. G06F 15/00
G06F 9/06
G06F 12/14

(21)Application number : 11-328802

(22)Date of filing : 18.11.1999

(71)Applicant : RICOH CO LTD

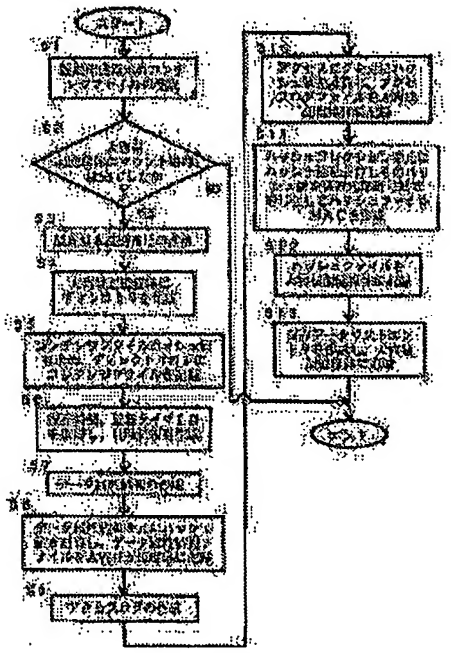
(72)Inventor : KANAI YOICHI
YANAIDA MASUYOSHI

(54) ELECTRONIC PRESERVING METHOD AND DEVICE FOR GUARANTEEING ORIGINALITY AND COMPUTER READABLE RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the complication of the procedure of the update or reference of a document in a device for preserving a composite document so that the originality can be guaranteed.

SOLUTION: At the time of receiving a plurality of contents files of an original to be newly prepared from the outside, a contents file hash value is calculated (S5). The hash value of data attribute information based on a new original identification number, data information, and contents file information is calculated and recorded (S8). Then, the hash value of the access log of the original is calculated and recorded (S10). Also, the hash value is calculated and enciphered based on hash collection obtained by combining the contents file hash value, the data attribute information hash value, and the access log hash value so that a hash file MAC can be prepared (S11). The hash collection is combined with the hash file MAC, and recorded in a large capacity storage medium (S12). Then, a preserved data list entry is prepared by combining the original identification number, the original attribute, the preparation date information, and the hash file MAC, and added to the large capacity storage medium (S13) to end the processing.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－147898
（P2001－147898A）
(43)公開日　平成13年５月29日(2001.5.29)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｚ	５Ｂ０１７
9/06	５５０	9/06	５５０Ｂ	５Ｂ０７６
12/14	３１０	12/14	３１０Ｚ	５Ｂ０８５

審査請求　未請求　請求項の数13　ＯＬ　（全 11 頁）

(21)出願番号　特願平11－328802

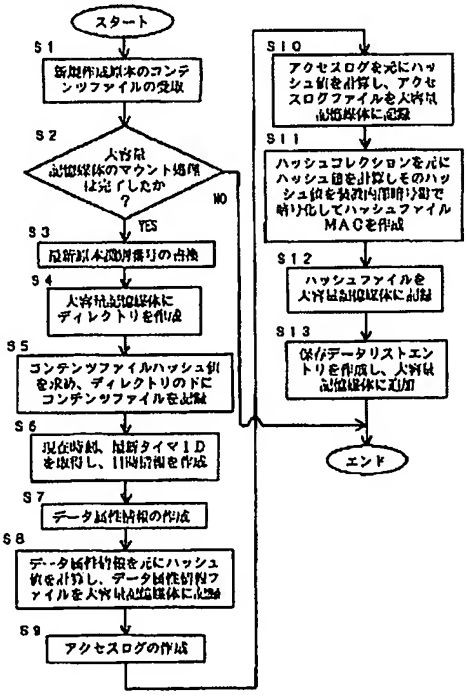
(22)出願日　平成11年11月18日(1999.11.18)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100079843
弁理士　高野　明近　（外２名）

最終頁に続く

(54)【発明の名称】　原本性保証電子保存方法、装置及びコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　複合文書を原本性を保証した形で保存する装置において、文書の更新，参照の手続の煩雑さを解消する。
【解決手段】　外部より新規に作成する原本の複数のコンテンツファイルを受け取ると、コンテンツファイルハッシュ値を計算する（Ｓ５）。新しい原本識別番号，日時情報，コンテンツファイル情報を元にしたデータ属性情報のハッシュ値を計算し記録する（Ｓ８）。この原本のアクセスログのハッシュ値を計算し記録する（Ｓ１０）。コンテンツファイルハッシュ値，データ属性情報ハッシュ値，アクセスログハッシュ値を合わせたハッシュコレクションを元にハッシュ値を計算して暗号化してハッシュファイルＭＡＣとする（Ｓ１１）。ハッシュコレクションとハッシュファイルＭＡＣを合わせて大容量記憶媒体に記録する（Ｓ１２）。原本識別番号，原本属性，作成日時情報，ハッシュファイルＭＡＣを合わせた保存データリストエントリを作成，追加して（Ｓ１３）処理を終了する。



1

【特許請求の範囲】

【請求項１】　記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、
外部から保存装置のプログラム終了要求を受け取ると、
該保存装置の内部記憶媒体に記録されている内部管理情報をすべて読み出し、
該読み出した内部管理情報を、前記保存装置内のマスター暗号鍵により暗号化し、
該暗号化した前記内部管理情報を前記内部記憶媒体に記録し、プログラムを終了する、
プログラム終了方法を含むことを特徴とする原本性保証電子保存方法。

【請求項２】　記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、
外部から保存装置のプログラム終了要求を受け取ると、
該保存装置の内部記憶媒体に記録されている、電子データの改ざん検知情報を算定するための装置暗号鍵及び該装置暗号鍵に対応する装置復号鍵を読み出し、
前記保存装置内のマスター暗号鍵により前記装置暗号鍵及び装置復号鍵を暗号化し、
該暗号化した装置暗号鍵及び装置復号鍵を前記内部記憶媒体に記録し、プログラムを終了する、
プログラム終了方法を含むことを特徴とする原本性保証電子保存方法。

【請求項３】　請求項１又は２に記載の原本性保証電子保存方法において、前記マスター暗号鍵は、前記プログラム内に保持されていることを特徴とする原本性保証電子保存方法。

【請求項４】　請求項１又は２に記載の原本性保証電子保存方法において、前記マスター暗号鍵は、前記保存装置にハードウェアで記憶されていることを特徴とする原本性保証電子保存方法。

【請求項５】　記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、
保存装置のプログラムが起動されると、
該保存装置の内部記憶媒体に記録されている、マスター暗号鍵により暗号化された内部管理情報を読み出し、
該マスター暗号鍵に対応するマスター復号鍵により、該暗号化された内部管理情報を復号し、
該復号された内部管理情報を該内部記憶媒体に記録する、
プログラム起動方法を含むことを特徴とする原本性保証電子保存方法。

【請求項６】　記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、
保存装置のプログラムが起動されると、
該保存装置の内部記憶媒体に記録されている、マスター暗号鍵により暗号化された、電子データの改ざん検知情報を算定するための装置暗号鍵及び該装置暗号鍵に対応する装置復号鍵を読み出し、

2

前記マスター暗号鍵に対応するマスター復号鍵により該暗号化された装置暗号鍵を復号し、装置暗号鍵とし、前記マスター復号鍵により該暗号化された装置復号鍵を復号し、装置復号鍵とし、
該復号した装置暗号鍵及び装置復号鍵を前記内部記憶媒体に記録し、
該内部記憶媒体に記録されている、前記記憶媒体を認証するための媒体認証コードリストを読み出し、
該媒体認証コードリストとともに記録されている改ざん検知コードを読み出し、
該改ざん検知コードと前記装置復号鍵を用いて該媒体認証コードリストの改ざんを検出する、
プログラム起動方法を含むことを特徴とする原本性保証電子保存方法。

【請求項７】　請求項５又は６に記載の原本性保証電子保存方法において、前記マスター暗号鍵及びマスター復号鍵は、前記プログラム内に保持されていることを特徴とする原本性保証電子保存方法。

【請求項８】　請求項５又は６に記載の原本性保証電子保存方法において、前記マスター暗号鍵及びマスター復号鍵は、前記保存装置にハードウェアで記憶されていることを特徴とする原本性保証電子保存方法。

【請求項９】　記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、
保存装置に前記記憶媒体がマウントされると、
該記憶媒体に記録されている、該記憶媒体を識別するための媒体識別番号を読み出し、
該記憶媒体の保存データリストファイルとともに記録されている改ざん検知コード（１）を読み出し、
前記保存装置の内部記憶媒体に記録されている、前記記憶媒体を認証するための媒体認証コードリストを読み出し、
該媒体認証コードリストから前記媒体識別番号に該当する媒体認証コードエントリを取り出し、
該媒体認証コードエントリにある改ざん検知コードが前記改ざん検知コード（１）と一致するかどうか検証し、
一致しなかった場合には、
マウントを解除し、
一致した場合には、
前記記憶媒体から前記保存データリストファイルを読み出し、
前記改ざん検知コード（１）と装置復号鍵を用いて該保存データリストファイルの改ざんを検出し、
改ざんが検出された場合にはマウントを解除し、
改ざんが検出されなかった場合にはマウントする、
記憶媒体マウント方法を含むことを特徴とする原本性保証電子保存方法。

【請求項１０】　記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、
外部から複数のコンテンツファイルを一つの原本として

3

新規に保存する要求を受け取ると、
すでに前記記憶媒体がマウントされていない場合には、
エラーを返して終了し、
前記記憶媒体がマウントされている場合には、
新しい原本に対応する属性情報を作成し、
該属性情報と受け取った複数のコンテンツファイルそれぞれについてハッシュ値を計算し、
該計算した複数のハッシュ値をまとめたハッシュリストを作成し、
保存装置内部に記憶している装置暗号鍵を用いて該ハッシュリストに対して改ざん検知コード（１）を計算し、
前記属性情報と複数のコンテンツファイルと該ハッシュリストと改ざん検知コード（１）を前記保存装置の前記記憶媒体に保存し、
該改ざん検知コード（１）を含む保存データエントリを作成し、
前記記憶媒体の保存データリストに該保存データエントリを追加し、
前記装置暗号鍵を用いて該保存データリストに対して改ざん検知コード（２）を計算し、
該改ざん検知コード（２）を該保存データリストとともに前記記憶媒体に記録し、
該改ざん検知コード（２）を含む媒体認証コードエントリを作成し、
前記保存装置の内部記憶媒体にある、前記記憶媒体を認証するための媒体認証コードリストに該媒体認証コードエントリを追加し、
前記装置暗号鍵を用いて該媒体認証コードリストに対して改ざん検知コード（３）を計算し、
該改ざん検知コード（３）を該媒体認証コードリストとともに前記内部記憶媒体に記録する、
原本を新規に保存するための方法を含むことを特徴とする原本性保証電子保存方法。

【請求項１１】　記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、
外部から保存装置に保存されている原本である電子データのコンテンツ読み出し要求を受け取ると、
すでに前記記憶媒体がマウントされていない場合には、
エラーを返して終了し、
前記記憶媒体がマウントされている場合には、
該記憶媒体から保存データリストファイルを読み出し、
該保存データリストファイルから、外部から指定された原本に該当する保存データエントリを取得し、
該保存データエントリにある改ざん検知コード（１）を取り出し、
前記外部から指定された原本に該当する電子データとともに前記記憶媒体に記録されているハッシュリストを読み出し、
該ハッシュリストに付与されている改ざん検知コード（２）を取り出し、

4

該改ざん検知コード（２）と前記改ざん検知コード（１）を比較し、同じ値でなければ該コンテンツ読み出し要求に対してエラーを返して終了し、同じ値であれば、該改ざん検知コード（２）と装置復号鍵を用いて該ハッシュリストの改ざんを検出し、
改ざんが検出された場合には前記コンテンツ読み出し要求に対してエラーを返して終了し、改ざんが検出されない場合には前記外部から指定されたコンテンツデータを前記記憶媒体から読み出し、
該読み出した該コンテンツデータに該当するハッシュ値（１）を前記ハッシュリストから取得し、
該コンテンツデータに対してハッシュ値（２）を計算し、
該ハッシュ値（２）と前記ハッシュ値（１）を比較し、同じ値でなければ前記コンテンツ読み出し要求に対してエラーを返して終了し、同じ値であれば、該コンテンツデータを該コンテンツ読み出し要求に対して返して終了する、
原本を参照するための方法を含むことを特徴とする原本性保証電子保存方法。

【請求項１２】　記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存装置において、
電子データを保存する記憶媒体と、
ネットワークを介して外部との通信を行うためのインターフェースである通信ポートと、
各種プログラムを実行するのに必要となるパラメータを記憶する内部記憶媒体と、
各種プログラムを格納するプログラム格納媒体と、
該プログラム格納媒体に格納された各種プログラムを読み出して実行するプロセッサとを有し、
前記プログラム格納媒体に請求項１乃至１１のいずれか１に記載の機能を有するプログラムを格納していることを特徴とする原本性保証電子保存装置。

【請求項１３】　請求項１乃至１１のいずれか１に記載の原本性保証電子保存方法を実行させるための、或いは、請求項１２に記載の原本性保証電子保存装置として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法、装置及び記録媒体に関し、より詳細には、複数のファイルから形成される複合文書の原本性を効率よく保証することができる原本性保証電子保存方法、装置及び記録媒体に関する。

【０００２】

【従来の技術】社会の高度情報化が進展するにつれ、従来は紙で保存が義務付けられていた書類も、電子的な保存できるようにすることが求められている。しかし、電

5

子文書は紙文書に比較して、痕跡を残さない改ざんが可能、不可視である、長期保存性が劣る、といった問題があるため、これらの問題が解決されなければ電子文書のまま原本として保存することは法的に許可されないという状況にある。

【０００３】この問題解決には３つのアプローチ、技術的解決（情報システム技術を駆使した解決）、組織的解決（運用規約を定め、組織的な運用による解決）、制度的解決（不正行為を法律で禁止するなど、社会システムによる解決）、がある。これら３つのアプローチを組み合わせることで問題を解決することになる。しかし、制度的な解決がなされるには時間がかかる上に、情報システムにおいては法律違反をしたことを突き止めるのが難しいという問題がある。また、組織的な解決の場合、その組織内での運用に不正がなかったことを証明することは難しいという問題がある。

【０００４】このような状況に対して、（特）情報処理振興事業協会では、創造的ソフトウェア育成事業の一環として平成９年度に「原本性保証電子保存システムの開発」プロジェクトを実施し、電子文書を原本として保存するための技術的解決手段を開発した。そのプロジェクトで開発された保存システムでは、電子文書の真正性、見読性、保存性を紙文書と同等のレベルで確保することを可能としている。

【０００５】真正性の確保としては、電子データが改ざんされた場合にはそれを検知することが可能にしており、さらにアクセスした履歴が残るようにしている。また、紙文書が原本とコピーを区別することができるように、電子データに対しても原本とそのコピーを区別することを可能にしている。そのことにより、どの電子データを保存義務のあるものとして取り扱っているのか明確にしている。注意しなければならないのはこの原本とコピーを区別する技術はコピープロテクトの技術や、著作権保護の技術とは異なるということである。原本である電子データの内容をどれだけコピーしても問題はないが、コピーはあくまでコピーとして扱われ、原本がどれであるか不明確になることを防いでいる技術である。

【０００６】見読性の確保については、保存装置と外部とのプロトコルを標準化し、そのプロトコルを通して確実に保存されている電子データが読み出せるようにしている。

【０００７】保存性の確保については、保存媒体にハードディスク等に比べて長期保存が可能な光ディスクを採用することを可能としており、その保存媒体が外部に取り出された際に、その媒体に対して不正な処理を施した場合にはそれを検知できるよう、処理している。

【０００８】この保存システムにより、電子データを原本として保存することが可能となり、電子データの証拠能力（証明力）を高めることが可能となっている。

【０００９】原本性保証電子保存方法及び装置の従来技術としては、特願平１１-０９０２１２号「原本性保証電子保存方法及び装置」、特願平１１-１４５３４０号「原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体」、特開平１０-２８３２６２号公報「ファイルシステムおよびプログラム記憶媒体」、小尾他：原本性保証電子保存システムの開発―基本機能の実現―,Medical Imaging Technology, Vol.１６,No.４, Proceedings of JAMIT Annual Meeting'９８(１９９８)、金井他：原本性保証電子保存システムの開発―システムの構築―,Medical Imaging Technology, Vol.１６, No.４, Proceedings of JAMIT Annual Meeting'９８(１９９８)、国分他：原本性保証電子保存システムの開発,（特）情報処理振興事業協会発行　創造的ソフトウェア育成事業及びエレクトロニック・コマース推進事業　最終成果発表会論文集　創造的ソフトウェア育成事業編(１９９８)、金井：原本性保証電子保存システムについて, Vol.３４, No.８,行政＆ＡＤＰ(１９９８)、がある。

6

【００１０】これらの技術を利用することで、電子データの原本性を保証することが可能となる。これにより、従来は紙による保存が法律上義務付けられていた原本書類が、電子データのまま原本として保存可能となり、高度情報化社会の推進に寄与することで社会全体の生産性が向上することが期待できる。

【００１１】

【発明が解決しようとする課題】これまでに開示されてきたこれらの従来技術は、どれも原本となる電子文書が一つのファイルであることを想定している。しかし、近年のWWW技術の普及により、ＨＴＭＬ，ＸＭＬ，ＳＧＭＬに見られるように電子文書は複数のファイルで構成される（以下、そのように複数のファイルで構成される電子文書を、「複合文書」と呼ぶ）ことが多くなってきている。そのような複合文書を、原本性を保証した形で保存するためには、従来開示されている技術を利用する場合には、それら複数のファイルを一つのファイルにまとめてから原本性保証電子保存装置に保存するか、各ファイルをそれぞれ別々の原本として原本性保証電子保存装置に保存するという方法を採らざるを得なかった。

【００１２】しかし前者の場合、どこからどこまでが最初のファイルとなるデータに相当し、どこからどこまでが次のファイルとなるデータに相当する、といったことを、原本性保証電子保存装置を利用する外部アプリケーションプログラムが管理し、記録しなければならないという面倒があった。さらに、原本性保証電子保存装置によってＣＤ－Ｒ等のリムーバブルメディアに原本データを記録した場合、そのリムーバブルメディアを他の一般的なＣＤ－Ｒドライブ等のドライブ装置にマウントした場合にも内容が読み出せた方が原本データの見読性を高められることになる。しかし、一つの原本として扱うた

めに一つの塊にまとめられたデータは、特殊なフォーマットとなってしまい、外部アプリケーションとして取り扱いにくいという問題があった。

【００１３】また、後者の場合、保存された各原本はもともと一つの文書を構成していた要素であるにも関わらず、それら各原本の関係が不明確になってしまい、それぞれ別々に管理され、編集されてしまうという問題があった。

【００１４】上記の問題を解決するために、特願平１１－１７３３７１号「原本性保証電子保存装置、原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体」では、複数のファイルで構成される複合文書を一つの原本データとして管理する機能を持ち、その原本データの原本性を保証することが可能な原本性保証電子保存方法及び装置が提供されている。

【００１５】しかしながら、特願平１１－１７３３７１号の発明においては、コンテンツごと、バージョンごとのハッシュ値の管理が複雑であるため、文書の更新・参照の手続きが煩雑になる傾向がある。

【００１６】本発明は、上述のごとき実情に鑑みてなされたものであり、複数のファイルで構成される複合文書を一つの原本データとして管理する機能を持ち、その原本データの原本性を保証することが可能な原本性保証電子保存方法、装置及び記録媒体において、文書のハッシュ値の管理を簡潔にすることを目的としたものである。また、本発明は、文書の更新，参照の手続きの煩雑さを解消すること、保存装置のプログラム起動，終了の処理についても安全性を高めるような処理方法、装置及び記録媒体を提供することをその目的とする。

【００１７】

【課題を解決するための手段】請求項１の発明は、記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、外部から保存装置のプログラム終了要求を受け取ると、該保存装置の内部記憶媒体に記録されている内部管理情報をすべて読み出し、該読み出した内部管理情報を、前記保存装置内のマスター暗号鍵により暗号化し、該暗号化した前記内部管理情報を前記内部記憶媒体に記録し、プログラムを終了する、プログラム終了方法を含むことを特徴としたものである。

【００１８】請求項２の発明は、記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、外部から保存装置のプログラム終了要求を受け取ると、該保存装置の内部記憶媒体に記録されている、電子データの改ざん検知情報を算定するための装置暗号鍵及び該装置暗号鍵に対応する装置復号鍵を読み出し、前記保存装置内のマスター暗号鍵により前記装置暗号鍵及び装置復号鍵を暗号化し、該暗号化した装置暗号鍵及び装置復号鍵を前記内部記憶媒体に記録し、プログラムを終了する、プログラム終了方法を含むことを特徴としたものである。

【００１９】請求項３の発明は、請求項１又は２に記載の原本性保証電子保存方法において、前記マスター暗号鍵は、前記プログラム内に保持されていることを特徴としたものである。

【００２０】請求項４の発明は、請求項１又は２に記載の原本性保証電子保存方法において、前記マスター暗号鍵は、前記保存装置にハードウェアで記憶されていることを特徴としたものである。

【００２１】請求項５の発明は、記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、保存装置のプログラムが起動されると、該保存装置の内部記憶媒体に記録されている、マスター暗号鍵により暗号化された内部管理情報を読み出し、該マスター暗号鍵に対応するマスター復号鍵により、該暗号化された内部管理情報を復号し、該復号された内部管理情報を該内部記憶媒体に記録する、プログラム起動方法を含むことを特徴としたものである。

【００２２】請求項６の発明は、記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、保存装置のプログラムが起動されると、該保存装置の内部記憶媒体に記録されている、マスター暗号鍵により暗号化された、電子データの改ざん検知情報を算定するための装置暗号鍵及び該装置暗号鍵に対応する装置復号鍵を読み出し、前記マスター暗号鍵に対応するマスター復号鍵により該暗号化された装置暗号鍵を復号し、装置暗号鍵とし、前記マスター復号鍵により該暗号化された装置復号鍵を復号し、装置復号鍵とし、該復号した装置暗号鍵及び装置復号鍵を前記内部記憶媒体に記録し、該内部記憶媒体に記録されている、前記記憶媒体を認証するための媒体認証コードリストを読み出し、該媒体認証コードリストとともに記録されている改ざん検知コードを読み出し、該改ざん検知コードと前記装置復号鍵を用いて該媒体認証コードリストの改ざんを検出する、プログラム起動方法を含むことを特徴としたものである。

【００２３】請求項７の発明は、請求項５又は６に記載の原本性保証電子保存方法において、前記マスター暗号鍵及びマスター復号鍵は、前記プログラム内に保持されていることを特徴としたものである。

【００２４】請求項８の発明は、請求項５又は６に記載の原本性保証電子保存方法において、前記マスター暗号鍵及びマスター復号鍵は、前記保存装置にハードウェアで記憶されていることを特徴としたものである。

【００２５】請求項９の発明は、記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、保存装置に前記記憶媒体がマウントされると、該記憶媒体に記録されている、該記憶媒体を識別するための媒体識別番号を読み出し、該記憶媒体の保存データリストファイルとともに記録されている改ざん検知コー

ド（１）を読み出し、前記保存装置の内部記憶媒体に記録されている、前記記憶媒体を認証するための媒体認証コードリストを読み出し、該媒体認証コードリストから前記媒体識別番号に該当する媒体認証コードエントリを取り出し、該媒体認証コードエントリにある改ざん検知コードが前記改ざん検知コード（１）と一致するかどうか検証し、一致しなかった場合には、マウントを解除し、一致した場合には、前記記憶媒体から前記保存データリストファイルを読み出し、前記改ざん検知コード（１）と装置復号鍵を用いて該保存データリストファイルの改ざんを検出し、改ざんが検出された場合にはマウントを解除し、改ざんが検出されなかった場合にはマウントする、記憶媒体マウント方法を含むことを特徴としたものである。

【００２６】請求項１０の発明は、記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、外部から複数のコンテンツファイルを一つの原本として新規に保存する要求を受け取ると、すでに前記記憶媒体がマウントされていない場合には、エラーを返して終了し、前記記憶媒体がマウントされている場合には、新しい原本に対応する属性情報を作成し、該属性情報と受け取った複数のコンテンツファイルそれぞれについてハッシュ値（圧縮コード）を計算し、該計算した複数のハッシュ値をまとめたハッシュリストを作成し、保存装置内部に記憶している装置暗号鍵を用いて該ハッシュリストに対して改ざん検知コード（１）を計算し、前記属性情報と複数のコンテンツファイルと該ハッシュリストと改ざん検知コード（１）を前記保存装置の前記記憶媒体に保存し、該改ざん検知コード（１）を含む保存データエントリを作成し、前記記憶媒体の保存データリストに該保存データエントリを追加し、前記装置暗号鍵を用いて該保存データリストに対して改ざん検知コード（２）を計算し、該改ざん検知コード（２）を該保存データリストとともに前記記憶媒体に記録し、該改ざん検知コード（２）を含む媒体認証コードエントリを作成し、前記保存装置の内部記憶媒体にある、前記記憶媒体を認証するための媒体認証コードリストに該媒体認証コードエントリを追加し、前記装置暗号鍵を用いて該媒体認証コードリストに対して改ざん検知コード（３）を計算し、該改ざん検知コード（３）を該媒体認証コードリストともに前記内部記憶媒体に記録する、原本を新規に保存するための方法を含むことを特徴としたものである。

【００２７】請求項１１の発明は、記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、外部から保存装置に保存されている原本である電子データのコンテンツ読み出し要求を受け取ると、すでに前記記憶媒体がマウントされていない場合には、エラーを返して終了し、前記記憶媒体がマウントされている場合には、該記憶媒体から保存データリストファイルを読み出し、該保存データリストファイルから、外部から指定された原本に該当する保存データエントリを取得し、該保存データエントリにある改ざん検知コード（１）を取り出し、前記外部から指定された原本に該当する電子データとともに前記記憶媒体に記録されているハッシュリストを読み出し、該ハッシュリストに付与されている改ざん検知コード（２）を取り出し、該改ざん検知コード（２）と前記改ざん検知コード（１）を比較し、同じ値でなければ該コンテンツ読み出し要求に対してエラーを返して終了し、同じ値であれば、該改ざん検知コード（２）と装置復号鍵を用いて該ハッシュリストの改ざんを検出し、改ざんが検出された場合には前記コンテンツ読み出し要求に対してエラーを返して終了し、改ざんが検出されない場合には前記外部から指定されたコンテンツデータを前記記憶媒体から読み出し、該読み出した該コンテンツデータに該当するハッシュ値（１）を前記ハッシュリストから取得し、該コンテンツデータに対してハッシュ値（２）を計算し、該ハッシュ値（２）と前記ハッシュ値（１）を比較し、同じ値でなければ前記コンテンツ読み出し要求に対してエラーを返して終了し、同じ値であれば、該コンテンツデータを該コンテンツ読み出し要求に対して返して終了する、原本を参照するための方法を含むことを特徴としたものである。

【００２８】請求項１２の発明は、記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存装置において、電子データを保存する記憶媒体と、ネットワークを介して外部との通信を行うためのインターフェースである通信ポートと、各種プログラムを実行するのに必要となるパラメータを記憶する内部記憶媒体と、各種プログラムを格納するプログラム格納媒体と、該プログラム格納媒体に格納された各種プログラムを読み出して実行するプロセッサとを有し、前記プログラム格納媒体に請求項１乃至１１のいずれか１に記載の機能を有するプログラムを格納していることを特徴としたものである。

【００２９】請求項１３の発明は、請求項１乃至１１のいずれか１に記載の原本性保証電子保存方法を実行させるための、或いは、請求項１２に記載の原本性保証電子保存装置として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体を特徴としたものである。

【００３０】

【発明の実施の形態】図１は、本発明における原本性保証電子保存装置（以下、「原本保存装置」と略して記述する）の構成を示す図で、この原本保存装置１００は、原本となる電子データを記憶し、ネットワークを介してホスト計算機１１０からアクセスされる装置であり、大容量記憶媒体１０１と、通信ポート１０２と、プログラム格納媒体１０３と、内部記憶媒体１０４と、タイマ１

０５と、プロセッサ１０６とからなる。外部システムはホスト計算機１１０側からネットワーク（一般的な通信路で構わない）を介して原本保存装置１００に対して電子データの保存・読み出し等を行う。通信ポート１０２は、ネットワークを介したホスト計算機１１０との通信をおこなうためのインターフェース部であり、たとえばＬＡＮカードなどの通信モデムなどからなる。

【００３１】大容量記憶媒体１０１は例えば光磁気ディスクやＣＤ－Ｒのように媒体そのものが原本保存装置１００から取り外し可能であっても構わないが、その他のブロックは原本保存装置１００として物理的に一体化されており、外部からのアクセスは通信ポート１０２を介する以外にない。各ブロックに対して直接アクセスする方法のない耐タンパー性を持った装置である。耐タンパー性を確保するレベルは筐体を開けられないようシールを貼る程度のものから、より高度に筐体を空けられてしまった場合には装置が動作しなくなるようなレベルまで考えられるが、そういった既存技術を利用する。プロセッサは規定のコマンドしか処理しないため、通信ポート１０２を介して内部に不正なアクセスをすることは不可能である。

【００３２】プログラム格納媒体１０３は、主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを格納したメモリであり、たとえば書換可能なＥＥＰＲＯＭや読み出し専用のＲＯＭなどからなる。

【００３３】内部記憶媒体１０４は、各種プログラムの実行に必要となるパラメータを記憶するＥＥＰＲＯＭなどからなるメモリであり、具体的には、装置暗号鍵、装置復号鍵、媒体認証コードリスト、最新データ識別番号、タイマ設定履歴ファイルおよびアカウント管理リストなどを記憶する。タイマ１０５は、プロセッサ１０６がプログラムの実行時に所得する時刻を計時するタイマである。

【００３４】プロセッサ１０６は、プログラム格納媒体１０３に格納された主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを読み出して実行する制御装置である。

【００３５】この原本保存装置１００の例では、プログラム格納媒体に鍵生成プログラム、暗号化プログラム、復号化プログラムなどを格納し、プロセッサによってそれらプログラムを実行する方式としているが、他にもそれら暗号処理を行うハードウェアモジュール、例えば暗号ＬＳＩボードなど、を原本保存装置１００に組み込み、そのハードウェアモジュールで鍵生成、暗号化、復号化の処理を行うようにしても良い。そのようなハードウエアの例としては、例えばＥＲＡＣＯＭ社（オーストラリア）のＣＳＡ７０００などが知られている。ここに例示したようなハードウェアを使用する場合には、ハードウェア内部に安全に鍵を保管することができるため、後の説明で使用するマスター暗号鍵およびマスター復号鍵を、このハードウェア内部に記憶させておくようにしても良い。

【００３６】この原本保存装置１００は外部システムから保存要求のあったデータを大容量記憶媒体１０１に記録するが、その際、後でデータの改ざんを検出するために、保存するデータに対して原本保存装置１００自身の秘密鍵によりメッセージ認証子（公開鍵暗号方式を採用する際には電子署名）を付加する。また、データそのものの不正な抹消を検出するために大容量記憶媒体１０１に記録されているデータのリストに対してもメッセージ認証子（ＭＡＣ：Message Authentication Code）を付加する。また、大容量記憶媒体１０１の不正なすり替え（過去の状態に戻すなど）を検出するために、大容量記憶媒体１０１の媒体識別番号と、その媒体のデータリストに対するメッセージ認証子のペアを原本保存装置１００内部に記録して管理する。また、データの作成日などに不正ができないよう、原本保存装置１００に内蔵されているタイマ１０５から現在時刻を取得し、データの属性として付与する。

【００３７】さらに、原本保存装置１００の内部で、オリジナルとコピーが区別できるよう、データに「仮原本」「原本」「謄本」といった属性を付与して管理している。「原本」の属性が付与されたデータに対して、外部から複製を要求すると、複製されたデータには「謄本」という属性が付与される。この属性は原本保存装置１００自身によって管理されており、外部から変更することはできない。大容量記憶媒体１０１を取り外して、外部でその属性を改ざんしても、後で原本保存装置１００にその大容量記憶媒体１０１を装着した際には改ざんが検出される。

【００３８】図２及び図３は、本発明による原本性保証電子保存装置において、原本を保証して保存されるデータ例の概念を示す図である。複数のコンテンツファイルで１つのバージョンを構成し、複数のバージョンと、文書の属性情報を記録しているデータ属性情報ファイル、アクセス履歴を記録しているアクセスログファイル、文書を構成する各ファイルのハッシュ値を管理するハッシュファイル、によって一つの保存データを構成し、管理する。

【００３９】図２では、バージョン１の段階で２つのコンテンツを持っており、バージョン２になる際に３つ目，４つ目のコンテンツが増え、バージョン３においては１番目のコンテンツ編集され、４番目のコンテンツが削除された様子を概念的に表している。薄い色で示したコンテンツは、コンテンツ属性情報のみが存在し、コンテンツデータファイルそのものは前のバージョンのコンテンツデータファイルを参照することを意味している。

【００４０】原本性を保証するための処理シーケンスに

13

ついて以下に説明する。

（処理の概要）原本保存装置１００の内部プログラム起動時に内部管理情報の正当性の検証を行い、各大容量記憶媒体１０１毎の認証コードが正しいことを確認する。そして、大容量記憶媒体１０１をマウントする際に大容量記憶媒体１０１に記録されている保存データリストの正当性の検証を行い、各保存データ毎のハッシュファイルＭＡＣが正しいことを確認する。そして、実際に大容量記憶媒体１０１に記録されている原本にアクセスする際には原本のコンテンツ、属性情報とともに管理されているハッシュファイルを用いてコンテンツ，属性情報，アクセスログの正当性の検証を行う。

【００４１】逆に、原本を作成したり更新したりした場合には原本の正当性を検証するためのハッシュファイルＭＡＣを計算し、原本とともに記録するだけでなく、大容量記憶媒体１０１の保存データリストにもそのハッシュファイルＭＡＣを記録する。マウントを解除する際にはその保存データリストを保護するために保存データリストの正当性を検証するためのリストＭＡＣを計算し、保存データリストとともに記録するだけでなく、原本保存装置１００内部の媒体認証コードリストにもそのリストＭＡＣを記録する。そして、原本保存装置１００の内部プログラムを終了する際には、媒体認証コードリストを保護するために、媒体認証コードリストを検証するための媒体認証コードリストＭＡＣを計算し、媒体認証コードリストとともに記録するとともに、その媒体認証コードリストＭＡＣの計算に使用した装置暗号鍵はプログラム内部に組み込まれているマスター暗号鍵によって暗号化して内部記憶媒体１０４に記録する。

【００４２】（プログラム起動処理）保存装置の内部プログラムが起動する際に、内部の管理情報の整合性を検証する。保存装置のサービスマンはプログラムを停止して内部をメンテナンスする可能性があるが、プログラムが停止していた間に内部に対して不正な改ざんが行われていないことを確認するため、内部記憶媒体１０４から媒体認証コードリストを読み出し、それに付与されている媒体認証コードリストＭＡＣの検証を行う。検証を行う前に、装置暗号鍵、装置復号鍵がマスター暗号鍵によって暗号化されているため、それを同じくプログラム内部に埋め込まれているマスター復号鍵で復号する。検証が失敗すれば、不正な改ざんが行われた可能性があるため、プログラムは起動せずに終了する。検証に成功すれば、媒体認証コードリストは信頼できることになり、プログラム起動が正常に行われる。

14

【００４３】（プログラム終了処理）プログラム終了時にはマウントしてある大容量記憶媒体１０１についてマウント解除処理を実行する。そして、内部記憶媒体１０４の媒体認証コードリストを読み出し、そのハッシュ値を計算して装置暗号鍵で暗号化し、媒体認証コードリストＭＡＣとする。媒体認証コードリストＭＡＣを媒体認証コードリストに付与し、内部記憶媒体１０４に記録する。また、内部記憶媒体１０４に記録してある装置暗号鍵や装置復号鍵は内部プログラムの中に埋め込まれているマスター暗号鍵で暗号化してから終了する。

【００４４】（大容量記憶媒体フォーマット処理）大容量記憶媒体１０１を利用可能にするためにはフォーマット処理が必要となる。新しい大容量記憶媒体１０１に媒体識別番号を振り、その媒体識別番号を媒体識別番号ファイルとして大容量記憶媒体１０１に記録する。空の保存データリストを作成し、その保存データリストに対するリストＭＡＣを計算して保存データリストに付与し、保存データリストファイルとして大容量記憶媒体１０１に記録する。そして、そのリストＭＡＣと媒体識別番号の組を媒体認証コードリストの新しいエントリとして内部記憶媒体１０４の媒体認証コードリストに追加する。媒体認証コードリストに対して媒体認証コードリストＭＡＣを計算し、媒体認証コードリストに付与して内部記憶媒体１０４に記録する。媒体認証コードリストに対してＭＡＣを付与する処理は、プログラム終了処理でのみ実行しても良い。媒体認証コードリストの構成を下表に示す。

【００４５】

【表１】

ハッシュファイル

ハッシュファイルMAC	
ハッシュエントリ #1	バージョン番号
	コンテンツ番号
	ハッシュ値
ハッシュエントリ #2	
ハッシュエントリ #3	
...	
ハッシュエントリ #N	

【００４６】（マウント処理）原本が保存された大容量記憶媒体１０１が装着されると、大容量記憶媒体１０１から媒体識別番号ファイルを読み出し、媒体識別番号を取得する。保存装置１００の内部記憶媒体１０４に記録されている媒体認証コードリストの中で、装着された大容量記憶媒体１０１に該当するエントリを参照し、リストＭＡＣを取得する。そのリストＭＡＣと、大容量記憶媒体１０１に記録されている保存データリストファイルに付与されているリストＭＡＣとを比較し、同じ値であるかどうかを検証する。同じ値でなければ、保存データリストファイルが不正であるため、マウント処理は失敗となる。同じ値であれば、大容量記憶媒体１０１から保

15

存データリストファイルを読み出し、保存データリストファイルのリストＭＡＣが正しいかどうか検証する。正しくない場合にはマウント処理は失敗となる。正しければ、保存データリストは信頼できることになり、マウント処理が成功となる。

【００４７】（マウント解除処理）大容量記憶媒体１０１のマウントを解除する際には、保存データリストファイルを元にハッシュ値を計算し、そのハッシュ値を装置暗号鍵で暗号化してリストＭＡＣとする。リストＭＡＣを保存データリストファイルに付与して大容量記憶媒体１０１に記録する。そして、内部記憶媒体１０４から媒体認証コードリストを読み出し、その中の、マウントを解除する大容量記憶媒体１０１の媒体識別番号に該当する媒体認証コードエントリについてリストＭＡＣを更新し、内部記憶媒体１０４に記録する。

【００４８】（原本参照）マウント処理が成功した後、大容量記憶媒体１０１に記録されている原本の参照が要求されると（具体的には原本識別番号を指定した参照要求を保存装置が受け取る）、保存データリストの中の該当する原本のエントリを参照し、ハッシュファイルＭＡＣを取得する。そのハッシュファイルＭＡＣと、大容量記憶媒体１０１に記録されている該当文書のハッシュファイルに付与されているハッシュファイルＭＡＣが同じ値であるかどうかを検証する。マウント処理の際に保存データリストの正当性は確認されているため、同じ値でなければ、ハッシュファイルが不正であるということになり、原本の参照処理は失敗する。同じ値であれば大容量記憶媒体１０１から該当文書のハッシュファイルを読み出し、ハッシュファイルのハッシュファイルＭＡＣが正しいかどうかを検証する。正しくない場合には原本参照処理は失敗となる。正しければ、ハッシュファイルは信頼できることになる。指定された原本のうち、例えば１番目のコンテンツファイルの参照が要求されているのであれば、１番目のコンテンツファイルに該当するハッシュ値をハッシュファイルから取り出し、そのハッシュ値がコンテンツファイルから計算されるハッシュ値と一致するかどうか検証する。すでにハッシュファイルの正当性は検証されているため、一致しなければコンテンツファイルが不正であることになり、原本参照処理は失敗となる。一致すれば、読み出したコンテンツファイルを要求元に渡し、原本参照処理が成功となる。

【００４９】（原本新規作成処理）図４は、本発明の実施形態における原本の新規作成方法を説明するためのフロー図である。原本保存装置１００の外部から新しい原本を新規に作成（保存）しようとする場合には以下のような処理になる。

【００５０】まず、外部より新規に作成する原本の複数のコンテンツファイルを受け取る（ステップＳ１）。大容量記憶媒体１０１のマウント処理が完了しているかを判断し（ステップＳ２）、未完了ならばエラー処理をして終了する。処理が完了しているならば、内部記憶媒体１０４の最新原本識別番号を読み出す。読み出した番号に１を加えて新しい最新原本識別番号とし、内部記憶媒体１０４に記録する（ステップＳ３）。その後、新しい最新原本識別番号を、この原本の原本識別番号とし、その番号を元にしてディレクトリ名を決定し、大容量記憶媒体１０１にディレクトリを作成する（ステップＳ４）。受け取ったコンテンツファイル個々についてハッシュ値を計算し、コンテンツファイルハッシュ値とし、作成したディレクトリの下に受け取ったコンテンツファイルを記録する（ステップＳ５）。

16

【００５１】次に、内部タイマ１０５より現在時刻を、内部記憶媒体１０４より最新タイマＩＤを取得し、現在時刻と最新タイマＩＤより日時情報を作成する（ステップＳ６）。先の新しい原本識別番号，日時情報，コンテンツファイル情報を元にデータ属性情報を作成する（ステップＳ７）。このデータ属性情報を元にハッシュ値を計算し、データ属性情報ハッシュ値とする。データ属性情報をデータ属性情報ファイルとして大容量記憶媒体１０１に記録する（ステップＳ８）。

【００５２】原本の新規作成を要求したユーザ名を含む、この原本のアクセスログを作成する（ステップＳ９）。このアクセスログを元にハッシュ値を計算し、アクセスログハッシュ値とする。アクセスログをアクセスログファイルとして大容量記憶媒体１０１に記録する（ステップＳ１０）。コンテンツファイルハッシュ値，データ属性情報ハッシュ値，アクセスログハッシュ値を合わせてハッシュコレクションとし、ハッシュコレクションを元にハッシュ値を計算して、そのハッシュ値を装置内部暗号鍵で暗号化し、ハッシュファイルＭＡＣとする（ステップＳ１１）。ここで、ハッシュコレクションとハッシュファイルＭＡＣを合わせて大容量記憶媒体１０１にハッシュファイルとして記録する（ステップＳ１２）。ハッシュファイルの構成を下表に示す。

【００５３】

【表２】

媒体認証コードリスト

媒体認証コードリスト MAC	
認証コードエントリ #1	媒体識別番号
	メッセージ認証子（リスト MAC）
認証コードエントリ #2	
認証コードエントリ #3	
...	
認証コードエントリ #N	

【００５４】ここで、バージョン番号が０でコンテンツ番号が１の場合にはデータ属性情報ファイルを意味する。バージョン番号が０でコンテンツ番号が２の場合にはアクセスログファイルを意味する。

【００５５】最後に、原本識別番号，原本属性，作成日時情報，ハッシュファイルＭＡＣを組み合わせて保存データリストエントリを作成し、大容量記憶媒体１０１の

17

保存データリストファイルに先の保存データリストエントリを追加して（ステップＳ１３）、処理を終了する。

【００５６】（原本コンテンツ更新処理）原本のコンテンツを更新する場合には、基本的に原本参照処理に記述されているような手順で保存されている原本の正当性を検証し、その上で原本新規作成処理と同様の手順でコンテンツの更新を行い、原本の正当性を検証するための改ざん検知コード等を計算して記録・管理するようにする。

【００５７】

【発明の効果】本発明の原本性保証電子保存方法及び装置によれば、文書のハッシュ値の管理を簡潔にでき、文書の更新，参照の手続きの煩雑さを解消できる。また、保存装置のプログラム起動，終了の処理についても安全性を高めることが可能である。

18

【図面の簡単な説明】

【図１】　本発明における原本保存装置の構成を示す図である。

【図２】　本発明による原本保存装置において、原本を保証して保存されるデータ例の概念を示す図である。

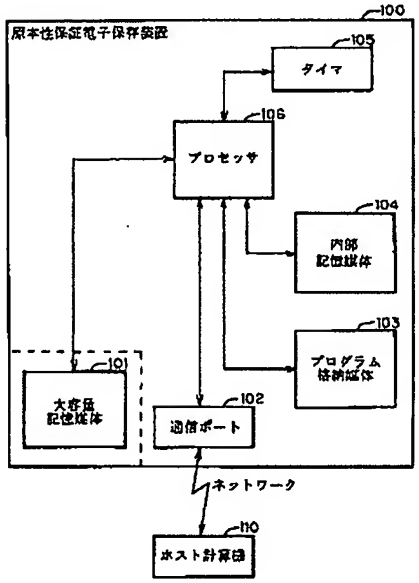
【図３】　本発明による原本保存装置において、原本を保証して保存されるデータ例の概念を示す図である。

【図４】　本発明の実施形態における原本の新規作成方法を説明するためのフロー図である。

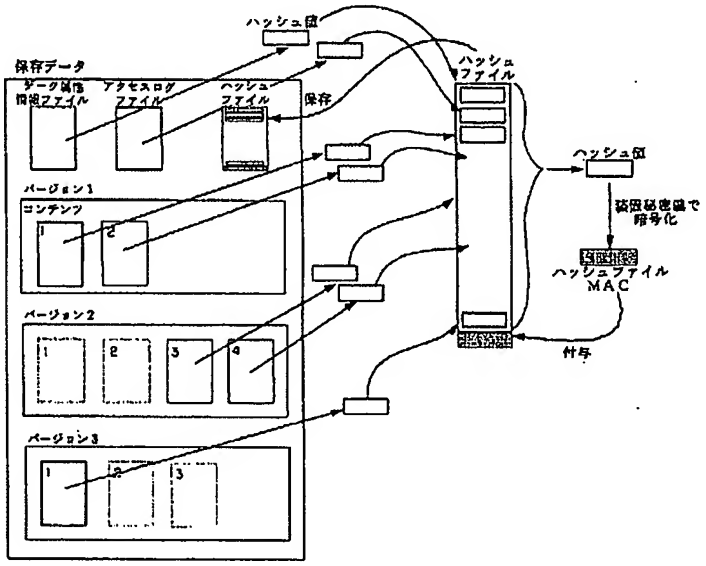
【符号の説明】

１００…原本保存装置、１０１…大容量記憶媒体、１０２…通信ポート、１０３…プログラム格納媒体、１０４…内部記憶媒体、１０５…タイマ、１０６…プロセッサ、１１０…ホスト計算機。

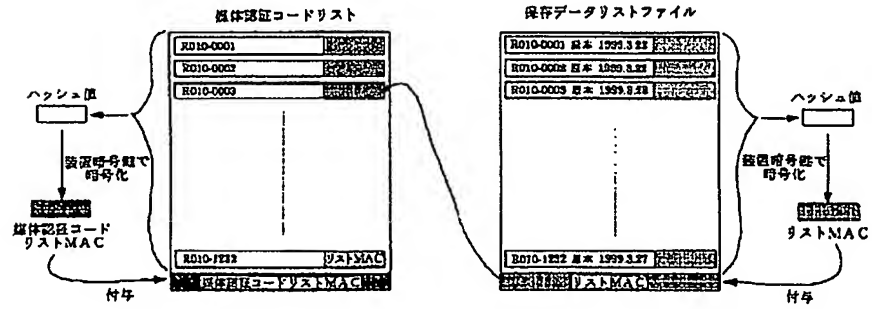
【図１】



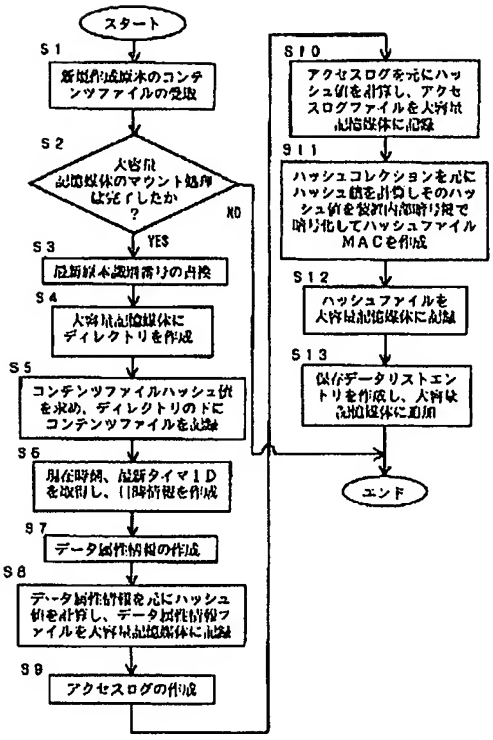
【図２】



【図３】



【図４】



フロントページの続き

Ｆターム(参考) 5B017 AA08 BA05 BA07 BB02 BB03
CA09 CA16
5B076 AB09 FA14 FA15 FA16
5B085 AE29